UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 09/01/2010

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
09/01/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *26-33 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-33 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response to the notices of non-compliant amendment was received on 09 June 2010. By this response, Claims 26 and 28 have been amended. Claims 1-25, 34-41, and 43 are canceled. No new claims have been added. Claims 26-33 and 42 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 04 December 2009 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 26-33 and 42 under 35 U.S.C. 101 as directed to non-statutory subject matter, Applicant argues that the amendments to independent Claim 26 have overcome the rejection by reciting a data carrier, and more specifically argues that the data carrier, semiconductor chip, and memory therein are "specifically tied to method steps recited in the body of the claim" that "do not merely involve 'insignificant post-solution activity'". This is alleged to tie the method to a machine as per the "machine or transformation" test of *In re Bilski* (see page 4 of the response received 04 December 2009). The Examiner respectfully disagrees.

With respect to the assertion that "the falsification and compensation steps are each performed on the semiconductor chip of the data carrier" (see page 4 of the present response), it is noted that neither the falsification nor the compensation step is

explicitly or implicitly claimed as performed on the semiconductor chip. The falsifying step is performed before execution of the operations on the semiconductor chip, but this does not explicitly limit the falsifying step itself to being performed on the semiconductor chip. Further, it is noted that there is no positive recitation within the claimed method of those operations actually being executed. Additionally, the combining step makes no mention of the semiconductor chip, data carrier, or memory, and therefore this step also does not require the machine, in contrast to Applicant's allegations.

Further, the recitations of the memory, semiconductor chip, and data carrier in the preamble do not serve to limit the method but only describe the intended use of the method. Additionally, the final "wherein" clause is only directed to insignificant extra-solution activity, namely that data are previously stored in the memory; however, this does not place any meaningful limit on the two positive steps of the method (the "falsifying" and "combining" steps). Rather, this prior storage of data only relates to the gathering of data to be used in the positive method steps, which is not central to the purpose of the claimed method. See, for example, the "Interim Examination Instructions for Evaluating Subject Matter Eligibility under 35 U.S.C. § 101", August 2009 (hereinafter "Interim Instructions"). The Interim Instructions explicitly describe gathering data as insignificant extra-solution activity (see page 6 of the interim instructions, last paragraph of section II.B., for example).

Therefore, in the absence of any clear indication in the claims that the method is not directed to an abstract idea, the method still appears to be directed to non-statutory subject matter.

Regarding the rejection of Claims 26-33 and 42 under 35 U.S.C. 103(a) as unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in view of Cordery et al, US Patent 5655023, Applicant generally argues that although Kocher discloses the steps of falsifying and combining as claimed, and Cordery does disclose pre-computation of secret data, the references cannot be combined to result in the claimed invention (see page 5 of the present response).

In response to applicant's argument that Cordery is nonanalogous art (see pages 5-6 of the present response), it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Cordery is concerned with the encryption and protection of secret data (see, for example, column 3, lines 18-58), which is reasonably pertinent to the problem with which Applicant is concerned, namely the prevention of leakage of secret information.

Applicant further argues that the function values of Cordery do not correspond to the function values of Kocher and are not stored with auxiliary values, and therefore, allegedly, the teachings of Cordery could not be used to modify the method of Kocher to obtain the claimed invention (pages 5-6 of the present response). In response to this argument, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references.

Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In particular, it is submitted that the disclosures in Kocher of the use of the blinding (i.e. the claimed falsifying) and the auxiliary data for compensating for the blinding/falsification (Kocher, paragraphs 0068, 0070, 0072, and 0073, as previously cited), in combination with the general teachings in Cordery of pre-computation and secure storage of security-related function values (Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see also column 4, lines 52-59, as previously cited), would have led one of ordinary skill in the art to the claimed invention, in order to protect the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13).

Applicant further argues that the secret data to be protected in Cordery is not stored on the data carrier but rather on a separate secure co-processor (see page 6 of the present response, citing Cordery, column 9, line 66-column 10, line 61, and Figure 5). However, Cordery does disclose that secret data is pre-computed and stored on data carriers (see, for example, column 4, lines 52-59, where pre-computed tokens are stored on smart cards, corresponding to the claimed data carrier). Further, the use of the secure co-processor in Cordery corresponds to the previous computation in safe surroundings as claimed (see Cordery, column 9, line 66-column 10, line 61, as cited, where the secure co-processor generates the tokens, and then the pre-computed tokens are transferred for storage to the storage device 104, corresponding to the claimed data carrier). It is noted that “safe surroundings” are not explicitly defined or

discussed in detail in the present specification, and therefore, the term has been broadly construed. It is certainly reasonable to conclude that a secure co-processor within tamper-proof surroundings would be considered "safe surroundings" for performing security-related calculations.

Applicant additionally argues that pre-computing the auxiliary data and function values as taught by Kocher would not have resulted in the claimed invention, would be contrary to the teachings of Kocher, and would make the resulting method less secure. In particular, Applicant argues that the security of Kocher depends on computation of the auxiliary data and function values after the performance of an operation step (pages 6-7 of the present response). However, Applicant does not appear to provide any evidence in support of at least this latter assertion. Applicant further states that the blinding is only performed after performing an additional permutation and that this is essential to the method of Kocher and cannot be omitted without rendering Kocher's method inoperative (pages 7-8 of the present response). However, there is nothing in Kocher to prevent the blinding data or the permutation data or both from being previously computed. Applicant appears to argue that the permutation could not be computed beforehand, but there is nothing that explicitly prevents this. Again, Cordery is seen as providing a general teaching that security related computations could be done prior to when they are needed in secure surroundings; therefore, this would be suggestive of pre-computing any of the needed function values, including, without limitation, the random blinding bit *b* and the random permutation *perm*, as well as the unblinding vector.

Applicant further argues that the blinding/falsifying operations in Kocher must be performed after the permutation and that interchanging their order would be contrary to the teachings of Kocher (page 8 of the present response). However, although the claim states that the falsifying is performed before execution of one or more operations, this does not preclude the performance of other operations prior to the falsifying step.

Applicant further details a list of changes that would allegedly need to be made to modify Kocher in order to obtain the claimed invention (page 9 of the present response); however, these changes all appear to be largely conjecture, and are further suggested by Cordery. Namely, the general teachings of Cordery would have suggested to one of ordinary skill that any number of security-related function values, such as the blinding bits and unblinding bits and any other data needed for these calculations such as the permutation could be pre-computed in secure surroundings and stored securely (Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see also column 4, lines 52-59, as previously cited), in order to protect the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13).

Additionally, Applicant again argues that the method of Kocher is "fundamentally different" than the claimed method (page 10 of the present response); however, Applicant has also acknowledged that Kocher discloses the two positively recited steps of the claimed method, namely the falsifying and combining/compensation (again, see page 5 of the present response). Therefore, the Examiner disagrees that the methods are fundamentally different. Further, Applicant again argues that Cordery only teaches pre-computation in the context of a secure co-processor (page 10 of the present

response); however, again, it is noted that this appears to correspond to the claimed limitation that the previous computation of the values is performed in "safe surroundings". Further, as noted above, Cordery is seen to teach, in general, the pre-computation of security-related function values, and in combination with the disclosed steps of Kocher, it is submitted that this would have suggested the claimed invention to one of ordinary skill in the art at the time the invention was made.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 26-33 and 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 26-33 and 42 are directed to methods as recited. While the claims recite a series of steps or acts to be performed, the claims are not clearly tied to a particular machine, nor do they transform underlying subject matter (such as an article or material) to a different state or thing. See *In re Bilski*, 545 F3d 943, 88 USPQ2d 1385, 1391 (Fed. Cir. 2008). The methods of Claims 26-33 and 42, and particularly independent Claim 26, generally include steps of "falsifying input data" and combining output data "to compensate for the falsification". These steps only describe calculations

being performed and do not clearly require any particular machine for the steps to be performed, nor is any transformation of an underlying article or material clearly apparent. The recitations in the preamble of a data carrier are only directed to the intended use of the method. The recitation that the falsification is performed "before execution" of operations "on the semiconductor chip" does not clearly limit the falsifying step itself. The recitation that data are previously stored in the memory of the semiconductor chip of the data carrier is only related to insignificant extra-solution activity. The lack of a machine or transformation weighs against patent eligibility of the method as directed solely to an abstract idea. Therefore, in the absence of further clear indications that the method is not directed to an abstract idea but rather to a practical application thereof, the claims are considered to be directed to a non-statutory abstract idea, and not to a statutory process. See also the Interim Guidance for Determining Subject Matter Eligibility for Process Claims in View of *Bilski v. Kappos*, 561 U.S. ____ (2010), published 27 July 2010, and see further the Interim Examination Instructions for Evaluating Subject Matter Eligibility under 35 U.S.C. § 101, dated 24 August 2009. It is further noted that the recitation of "a memory of a data carrier" in dependent Claim 28, while appearing to be directed to a particular machine, only relates to insignificant extra-solution activity, namely the storage of data, and therefore, the presence of the memory of the data carrier is not sufficient to clearly limit Claim 28 to a statutory process. Therefore, the claims are not directed to statutory subject matter.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 26-33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in view of Cordery et al, US Patent 5655023.

In reference to Claim 26, Kocher discloses a method of protecting secret data stored in a semiconductor chip of a data carrier, where the method includes falsifying input data by combination with auxiliary data before execution of one or more operations (paragraphs 0068, 0070, and 0072, where blinding occurs before permutation operations), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data (paragraphs paragraphs 0070, 0072, and 0073, where unblinding occurs to compensate for the blinding), where the auxiliary value was determined by executing the operations using the auxiliary data as input data (paragraph 0072, where the output buffer is initialized with the blinding bit and the data in the output buffer is the result of using the input permutation table, i.e. the operations). However, while Kocher discloses previously determining the auxiliary data and/or values (see paragraph 0072), Kocher does not explicitly disclose determining the auxiliary value previously and in safe surroundings.

Cordery discloses a method in which secret function values are pre-computed in safe surroundings and where the secret values are maintained securely, i.e. stored in the memory of a semiconductor chip of a data carrier (see column 3, lines 18-25, where tokens are pre-computed, see also column 5, lines 10-12, where tokens include encrypted data, and column 3, lines 11-13, where the encryption algorithm and keys are protected; see also column 4, lines 52-59, where the tokens are stored on smart cards and protected against tampering, i.e. maintained securely). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kocher to include pre-computation and safe storage of secret function values in order to protect the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13).

In reference to Claim 27, Kocher and Cordery further disclose that the combination with the auxiliary function value is performed before execution of a non-linear operation (see Kocher, paragraph 0074, where inputs can be maintained in a blinded state and only reconstituted when nonlinear operations must be performed).

In reference to Claim 28, Kocher and Cordery further disclose that the auxiliary data are varied and function values are stored in the memory of the data carrier (Kocher, paragraphs 0072-0075; Cordery, column 4, lines 54-58).

In reference to Claims 29-32, Kocher and Cordery further disclose that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (see Kocher, paragraphs 0072 and 0075).

In reference to Claim 33, Kocher and Cordery further disclose combining the output data and auxiliary function value using an XOR operation (see Kocher, paragraph 0073).

In reference to Claim 42, Kocher and Cordery further disclose that operations include permutations of data (see Kocher, paragraphs 0068 and 0070-0074).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2437